

CLAIMS (None Currently Amended)

1. (Previously Presented) A system for managing client accounts and controlling access to resources over data networks, said system comprising:

(a) a mechanism for sharing client information and charges among a plurality of service providers;

(b) a client registration database maintained by one of the service providers (its "home provider") and includes information which selectively authorizes access to the resources of the other service providers ("outside providers"), each service provider maintaining an independent database of its respective clients;

(c) a settling means, separate from a respective home provider, for settling accounts among service providers by charging the home provider for access by its clients to the resources of the outside providers, the settling means accessing a respective home provider registration database, and communicating with an accounting database maintained separately from a respective registration database;

(d) a payment means adapted to assure that the outside providers are then paid for that access;

(e) a sharing means adapted to allow the service providers to share users without requiring an open account for each user at each service provider; and

(f) a verification means including a token and an authentication server adapted to allow each service provider to determine if a particular client is registered by a home provider, verify that the client has authenticated at his home provider, and determine that client's access privileges and criteria.

2. (Previously Presented) A system as recited in claim 1 including means by which an owner of goods sells access to those goods across a data network such that the owner may instantaneously and simultaneously display across the network multiple differing prices of the same good or classes of goods.

3. (Previously Presented) A system as recited in claim 1, including means by which a service provider instantaneously configures the form and substance of services or goods across

a data network provided to different or unique clients in response to data accompanying the client's request for service.

4. (Previously Presented) A system as recited in claim 1, including means by which a service provider instantaneously determines whether or what type or form of service or goods across a data network to provide to different or unique clients based upon data about the client provided along with the client's request for service.

5. (Previously Presented) A system as recited in Claim 1, including means by which multiple service providers aggregate, transfer and share data about the clients, in a standardized form which identifies each client by a unique alpha-numeric sequence, but where the personal identifying attributes of the client need be known only to the home provider.

6. (Previously Presented) A system as recited in Claim 1, including means by which a service providers request access to, review of, or purchase of resources or goods across a data network of clients on the basis of specific attributes of the client which the client elects to provide at the moment when service is requested, where such attributes are technically capable of being an integral and automatic part of the request form.

7. (Previously Presented) A system as recited in Claim 1, including means by which a home provider provides a client's preference, pricing and service-class information to a common service point in exchange for an authenticatable token, which the home provider then provides to its client, so that the client may in turn offer the token to multiple outside providers whose services or goods across a data network the client wishes to access, review or purchase.

8. (Original) A system as recited in Claim 7, which employs the Internet's Hyper-Text Transfer Protocol (HTTP), and has appending means adapted to appending to or include in the user computer a Uniform Resource Locator (URL), or in a Request/Response Header, a sequence of alpha-numeric characters which includes said authenticatable token.

9. (Previously Presented) A system as recited in Claim 7, which includes an acceptance means by which a client's token is accepted by a service provider from whom the client wishes to receive services or goods across a data network, and is instantaneously submitted to the common service point, which, if the token's contents match that of a token in the common service point's dynamic session database, returns preference, pricing and service-class information about the requesting client, prior to the providing of the requested services or goods across a data network.

10. (Original) A system as recited in Claim 9, of utilizing the User Datagram Protocol (UDP) for implementing the acceptance means.

11. (Previously Presented) A system as recited in Claim 1, for collecting and storing at a common service point discrete records of access by clients to resources or goods across a data network of multiple service providers, where such collection is capable of occurring instantaneously subsequent to the providing of each resource or good.

12. (Previously Presented) A system as recited in Claim 11, including means by which discrete records are instantaneously sorted and stored in databases according to the identity of the home provider.

13. (Previously Presented) A system as recited in Claim 1, including means for collecting and aggregating records of financial charges for access to, review or acquisition of services or goods across a data network such that the records may be supplied to the suppliers of client servers without knowledge of or reference to the ultimate form of payment by the client.

14. (Previously Presented) A system as recited in Claim 1, in which said token is only "read" by said authentication server, thus permitting the token to be private-key encrypted.

15. (Previously Presented) A system as recited in Claim 1, wherein which said client comprises an end user and has an end user's account and an end user's account manager, for enabling an initiating Internet World Wide Web host to present in HyperText Markup Language

(HTML) "hypertext links" which address services or goods available from multiple other receiving World Wide Web sites such that when the end user highlights or clicks the link a process is initiated whereby the receiving site is able to bill the end user's account manager for access to, review or acquisition of the services or goods, without regard to whether the end user's account is maintained by the initiating WWW host or by some other service provider.

16. (Previously Presented) A system as recited in Claim 1, which includes a sequence means adapted for obtaining, transferring and maintaining among multiple service providers a unique alpha-numeric sequence associated with a specific digital information resource or object for a purpose; where the topological location of the resource on the network may not necessarily be related or relevant to the location where, or time when, the resource was originally created.

17. (Previously Presented) A system as recited in Claim 1, which includes a sequence means adapted for obtaining, transferring and maintaining among multiple service providers a dynamically updated record of funds encumbered by a network user for the purchase of a digital information resource or resources, such that each subsequent record of purchase in time, and the transfer to clients of an updated record of funds available or authorized to be encumbered, is accomplished.

18. (Previously Presented) A method for managing client accounts and controlling access to resources over data networks, said method comprising:

- (a) sharing client information and charges among a plurality of service providers;
- (b) registering a client with one of the service providers (the "home provider") in a registration database, and allowing the client to access the resources of the other service providers ("outside providers"), each service provider maintaining an independent registration database of its clients;
- (c) settling accounts among service providers by charging the home provider for access by its clients to the resources of the outside providers, by accessing a respective home provider registration database, and communicating with an accounting database maintained separately from a respective registration database;

(d) assuring that the outside providers are paid for access by of a home provider for a client's access to the outside provider's resources;

(e) allowing the providers to share users without requiring an open account for each user at each service provider; and

(f) allowing each provider to determine if a particular client is registered, verifying that the client has authenticated at his home provider, and determining that client's access privileges and criteria.

19. (Previously Presented) A method as recited in claim 18 by which the owner of goods sells access to those goods across a data network such that the owner may instantaneously and simultaneously display across the network multiple differing prices of the same good or classes of goods.

20. (Previously Presented) A method as recited in claim 18, by which a service provider instantaneously configures the form and substance of services or goods across a data network provided to different or unique clients in response to data about the client accompanying the client's request for service.

21. (Previously Presented) A method as recited in claim 18, by which a service provider instantaneously determines whether or what type or form of service or goods across a data network to provide to different or unique clients based upon data about the client accompanying the client's request for service.

22. (Previously Presented) A method as recited in Claim 18, by which multiple service providers aggregate, transfer and share data about the clients, in a standardized form which identifies each client by a unique alpha-numeric sequence, but where the personal identifying attributes of the client need be known only to the home provider.

23. (Previously Presented) A method as recited in Claim 18, in which a service provider requests access to, review of, or purchase of resources or goods across a data network on the basis of specific attributes of the client which the client elects to provide at the moment

when service is requested, where such attributes are technically capable of being an integral and automatic part of the request form.

24. (Previously Presented) A method as recited in Claim 18, in which a home provider provides a client's preference, pricing and service-class information to a common service point in exchange for an authenticatable token, which the home provider then provides to its client, so that the client may in turn offer the token to multiple outside providers whose services or goods across a data network the client wishes to access, review or purchase.

25. (Original) A method as recited in claim 24, employing the Internet's Hyper-Text Transfer Protocol (HTTP), of appending to or including in a Uniform Resource Locator (URL), or in a Request/Response Header, a sequence of alpha-numeric characters which includes said authenticatable token.

26. (Previously Presented) A method as recited in claim 24, which includes an acceptance step by which a client's token is accepted by a service provider from whom the client wishes to receive services or goods across a data network, and is instantaneously submitted to the common service point, which, if the token's contents match that of a token in the common service point's dynamic session database, returns preference, pricing and service-class information about the requesting client, prior to the providing of the requested services or goods across a data network.

27. (Original) A method as recited in claim 26, of utilizing the User Datagram Protocol (UDP) to accomplish the acceptance step.

28. (Previously Presented) A method as recited in claim 18, for collecting and storing at a common service point discrete records of access by clients to resources or goods across a data network of multiple service providers, where such collection is capable of occurring instantaneously subsequent to the providing of each resource or good.

29. (Original) A method as recited in claim 28, by which discrete records are instantaneously sorted and stored in databases according to the identity of the service provider of the individual client whose activity resulted in the record being produced.

30. (Previously Presented) A method as recited in Claim 18, for collecting and aggregating records of financial charges for access to, review or acquisition of services or goods across a data network such that the records may be supplied to the suppliers of client services without knowledge of or reference to the ultimate form of payment by the client.

31. (Previously Presented) A method as recited in Claim 18, in which said token is only "read" by said authentication server, thus permitting the token to be private-key encrypted.

32. (Previously Presented) A method as recited in claim 18, wherein which said client comprises an end user and has an end user's account and an end user's account manager, for enabling an initiating Internet World Wide Web host to present in HyperText Markup Language (HTML) "hypertext links" which address services or goods available from multiple other receiving World Wide Web sites such that when the end user highlights or clicks the link a process is initiated whereby the receiving site is able to bill the end user's account manager for access to, review or acquisition of the services or goods, without regard to whether the end user's account is maintained by the initiating WWW host or by some other service provider.

33. (Previously Presented) A method as recited in claim 18, including the step of obtaining, transferring and maintaining among multiple service providers a unique alpha-numeric sequence associated with a specific digital information resource or object for a purpose; where the topological location of the resource on the network may not necessarily be related or relevant to the location where, or time when, the resource was originally created.

34. (Previously Presented) A method as recited in Claim 18 which includes sequence steps for obtaining, transferring and maintaining among multiple service providers a dynamically updated record of funds encumbered by a client for the purchase of a digital information resource

or resources such that each subsequent record of purchase in time, and the transfer to clients of an updated record of funds available or authorized to be encumbered, is accomplished.

35. (Previously Presented) A method of providing an online service to a user over a public network, the online service provided by a Service Provider (SP) site to a user computer via the public network, the method comprising the steps of:

- sending a request message from the user computer to the SP site over the public network to request the use of the online service;

- generating a challenge message at the SP site in response to the request message and sending the challenge message over the public network to the user computer;

- generating a response message in the user computer in response to the challenge message and sending the response message over the public network to the SP site, the response message including or being based upon an identifier of the user;

- sending at least the response message from the SP site to a remote online broker site, the online broker site having a brokering database which contains account information of registered users of an online brokering service of the online broker site;

- processing the response message at the remote online broker site to determine whether the response message is authentic, the step of processing comprising accessing the account information in the brokering database;

- sending a verification message from the remote online broker site to the SP site, the verification message indicating whether the response message is authentic;

- retrieving access rights data of the user from the brokering database if the response message is authentic, the access rights data specifies a plurality of content categories to which the user has access, the plurality of content categories corresponding to a plurality of different online services offered by the SP site;

- sending the access rights data from the online broker site to the SP site;

- providing the online service from the SP site to the user computer over the public network if the verification message indicates that the response message is authentic;

- denying access by the user to the online service if the verification message indicates that the response message is not authentic; and

- updating a settling database at a settlor site, with a charge related to the user computer

access to the SP site, the settlor site being maintained separately from the remote online broker site.

36. (Previously Presented) A method as in claim 35, wherein the step of generating a response message comprises obtaining a password of the user.

37. (Previously Presented) A method as in claim 36, wherein the step of generating the response message further comprises applying a cryptographic algorithm to at least the challenge message such that the resulting response message depends upon both the challenge message and the password.

38. (Previously Presented) A method as in claim 36, wherein the step of obtaining the password of the user comprises retrieving the password from a password cache on the user computer, the password cache temporarily storing the password following manual entry by the user, the method thereby enabling the user to access multiple SP sites without re-entering the password.

39. (Previously Presented) A method as in claim 35, further comprising the steps of:

assigning an anonymous identifier to the user at the online broker site and sending the anonymous identifier to the SP site to enable the SP site to anonymously charge the user for an online service; and

generating a billing event at the SP site and sending the billing event to the settlor site, the billing event specifying at least (1) the anonymous identifier of the user, and (2) a monetary charge to be applied to an account of the user.

40. (Previously Presented) A method as in claim 35, further comprising the steps of:

establishing a connection between the user computer and the settlor site; and

providing an online billing statement to the user over the connection, the online billing statement reflecting the monetary charge specified in the billing event.

41. (Previously Presented) A method as in claim 35, further comprising the step of sending a billing statement from the settlor site to the user computer over the public network, the billing statement reflecting the monetary charge specified in the billing event.

42. (Previously Presented) A method as in claim 35, further comprising the steps of:

sending an access rights update request from the SP site to the remote online broker site, the access rights update request specifying an update to be made by the online brokering service to the access rights of the user; and

processing the access rights update request at the online broker site by updating the access rights data of the user stored within the brokering database.

43. (Previously Presented) A method as in claim 35, further comprising the steps of:

retrieving user-specific preference data of the user from the brokering database and sending the preference data from the online broker site to the SP site, the preference data indicating at least one user-specified preference for the customization of online services; and

adjusting the online service provided from the SP site according to the user-specified preference.

44. (Previously Presented) A method as in claim 43, wherein the preference data includes a connection speed at which the user computer connects to the public network, and wherein the step of adjusting comprises providing the service to the user computer at a speed which is commensurate with the connection speed.

45. (Previously Presented) A method as in claim 43, wherein the preference data includes a display preference for the display of a particular type of media.

46. (Previously Presented) A method as in claim 35, further comprising the steps of: generating a first session key at the user computer;

generating a second session key at the online broker site and sending the second session key to the SP site, the second session key corresponding to the first session key; and

using the first and second session keys to encrypt and decrypt message traffic between the user computer and the SP site as the online service is provided to the user computer.

47. (Previously Presented) A method as in claim 35, wherein the public network comprises the Internet.

48. (Previously Presented) A method as in claim 35, wherein the steps of passing the request, challenge and response messages over the public network respectively comprise passing the request, challenge and response messages over a private network.

49. (Previously Presented) A method providing a fee-based online service from a Service Provider (SP) site to a user over a public network while concealing the payment and personal information of the user from the Service Provider, comprising the steps of:

registering a user at a registration site that provides a registration service, the registration site having a registration database which contains registration information on the user and on other users of the online service, the registration site being located remotely from the SP site;

providing an online broker site that provides an online brokering service, the online broker site having a brokering database which contains account information on the user and on other users of the online brokering service, the online broker site being located remotely from the SP site and the registration site;

establishing a connection between a computer of the user ("user computer") and the SP site over at least the public network;

generating an encrypted authentication message at the user computer and sending the authentication message to the registration site via at least the public network;

verifying the authentication message at the registration site to thereby authenticate the user, the step of verifying comprising accessing the account information of the user stored in the registration database;

generating an anonymous ID at the registration site and sending the anonymous ID to the SP site to allow the SP site to impose a charge the user for the online service;

providing the online service from the SP site to the user computer over the public network;

generating a billing event at the SP site and sending the billing event to the online broker site, the billing event specifying at least (1) the anonymous ID, and (2) a monetary charge to be applied to an account of the user in the brokering database.

50. (Previously Presented) A method as in claim 49, wherein the step of generating an encrypted authentication message comprises the steps of prompting the user for a password and using the password to generate the authentication message, the password stored in the registration database to permit determination whether the authentication message corresponds to the password.

51. (Previously Presented) A method as in claim 49, wherein the step of sending the encrypted authentication message to the online broker site comprises the steps of:
sending the authentication message from the user computer to the SP site over the public network; and
sending the authentication message from the SP site to the registration site.

52. (Previously Presented) A method as in claim 49, further comprising the step of processing the billing event at the online broker site to thereby apply the charge to the account of the user.

53. (Previously Presented) A method as in claim 52, further comprising the step of providing an account statement from the online broker site to the user computer over at least the public network, the account statement reflecting the charge specified in the billing event.

54. (Previously Presented) A method as in claim 49, further comprising the steps of:

retrieving access rights data of the user from the brokering database, the access rights data specifying the access rights of the user with respect to the online service and/or the SP site; and

sending the access rights data from the online registration site to the SP site.

55. (Previously Presented) A method as in claim 54, further comprising the step of interpreting the access rights data at the SP site to determine whether the user is authorized to access a particular content item of the SP site.

56. (Previously Presented) A method as in claim 54, further comprising the step of sending an access rights update request from the SP site to the registration site, the access rights update request specifying at least (1) the anonymous ID of the user, and (2) an update to be made to the access rights data of the user.

57. (Previously Presented) A method as in claim 49, further comprising the steps of:

retrieving user-specific customization data of the user from the brokering database and sending the customization data from the online broker site to the SP site, the customization data indicating a user-specified preference for the customization of the online service; and

adjusting the online service provided from the SP site according to the user-specified preference.

58. (Previously Presented) A method as in claim 57, wherein the customization data includes at least one of a display preference for the display of a particular type of media and a connection speed at which the user computer connects to the public network, and wherein the step of adjusting comprises providing the service to the user computer at a speed which generally corresponds to the connection speed.

59. (Previously Presented) A method as in claim 49, further comprising the steps of:

generating a first session key at the user computer;

generating a second session key at the registration site and sending the second session key to the SP site, the second session key corresponding to the first session key; and

using the first and second session keys to encrypt and decrypt message traffic between the user computer and the SP site as the online service is provided to the user computer.

60. (Previously Presented) A method as in claim 49, wherein the public network comprises the Internet.

61. (Previously Presented) A method as in claim 49, wherein the online service comprises a software download service.

62. (Previously Presented) A method as in claim 49, wherein the online service comprises user access to media content.

63. (Previously Presented) A system for allowing users to securely access online service providers over an untrusted distributed network, comprising:

a plurality of Service Provider (SP) sites connected to the distributed network, each SP site running at least one service application to provide an online service to users over the distributed network;

a plurality of user computers connected to the distributed network, each user computer running at least one client application for accessing online services of the SP sites;

an online broker site connected to the plurality of SP sites, the online broker site running at least one brokering application to provide an online brokering service to account for use of the online services by respective users, the SP sites optionally including a user database containing user-specific authentication information of users that have registered with an SP site, the registered users accessing the SP sites from the users computers over the distributed network; and

an authentication protocol for allowing the SP site to authenticate registered users in response to user-specific authentication requests from the SP sites, the authentication requests responsive to requests from the user computers to access the online services of the SP sites, the

authentication protocol implemented by software components of the user computers, the SP sites, and the online broker site.

64. (Previously Presented) A system as in claim 63, further comprising a billing system for allowing the SP sites to charge the registered users for accesses to the online services by sending billing events to the online brokering service, the billing system including a centralized database for recording billing events to accounts of the registered users.

65. (Previously Presented) A system as in claim 64, wherein the billing system includes a billing viewer application running on the user computers, the billing viewer application allowing a registered user to view a personal billing statement stored in the online broker database, the billing statement including charges from multiple different SP sites of the plurality of SP sites.

66. (Previously Presented) A system as in claim 63, further comprising an access rights database at the registration site, the access rights database storing access rights data for a plurality of the registered users, the access rights data specifying access rights of the plurality of registered users with respect to the SP sites, the access rights data provided to the SP sites by the registration site.

67. (Previously Presented) A system as in claim 63, wherein the authentication protocol implements a challenge-response protocol.

68. (Previously Presented) A system as in claim 63, wherein the distributed network comprises the Internet.

69. (Previously Presented) A method providing a fee-based online service from a Service Provider (SP) site to a user over a distributed network while concealing the payment and personal information of the user from the Service Provider, comprising the steps of:

providing a registration site that provides a registration service, the registration site having a registration database which contains registration information on the user and on other users of the online service, the registration site being located remotely from the SP site;

providing an online broker site that provides an online brokering service, the online broker site having a brokering database which contains account information on the user and on other users of the online brokering service, the online broker site located remotely from the SP site and the registration site;

sending an access request from a computer of the user ("user computer") over the distributed network to the SP site;

sending an authentication request from the SP site to the registration site in response to the access request;

prompting the user for a user identifier at the user computer and sending the user identifier to the registration site;

authenticating the user at the registration site in response to the authentication request, the step of authenticating comprising using the user identifier sent from the user computer to access the account information stored within the registration database;

sending a verification message from the registration site to the SP site in response to the authentication request, the verification message indicating whether the step of authenticating was successful;

retrieving access rights data of the user from the registration database if the step of authenticating is successful, the access rights data specifying a plurality of access rights of the user with respect to the online service and/or the SP site;

sending the plurality of access rights data from the registration site to the SP site to anonymously inform the SP site of the access rights of the user;

providing the fee-based online service from the SP site to the user computer over the distributed network only if the verification message indicates that the step of authenticating was successful;

generation a billing event at the SP site and sending the billing event to the online broker site, the billing event anonymously identifying the user to the online brokering service, the billing event including a charge for the providing of the online service to the user computer; and

updating an account of the user at the online broker site to reflect the charge included within the billing event.

70. (Previously Presented) A method as in claim 69, further comprising the step of providing an account statement from the online broker site to the user computer over at least the distributed network, the account statement reflecting the charge included in the billing event.

71. (Previously Presented) An online brokering service for allowing users of a public network to anonymously purchase online services from Service Provider (SP) sites on the public network, the online brokering service provided from an online broker site and a registration site that are each located separately and remotely from the SP sites, the online brokering service comprising:

- a database at the registration site which contains account information of users that have registered with online brokering service, the account information including at least a unique identifier of each registered user;

- a billing system at the online broker site for recording monetary charges to accounts of registered users, the monetary charges corresponding to online services purchased from the SP sites over the public network;

- a software package running at the online broker site, the brokerage software package performing at least the following functions:

- (a) receiving identifying information about the user generated at the registration site to correlate an anonymous ID of a registered user with an identification of an account of a registered user;

- (b) receiving user-specific billing events from the SP sites and passing the billing events to the billing system to update the accounts of registered users, each billing event specifying at least (1) an anonymous ID of a registered user, and (2) a charge to be applied to the account of the registered user; and

- a software package running at the registration site, the registration software package performing at least the following functions:

(a) authenticating registered users in response to authentication requests received from the SP sites, the authentication requests generated in response to attempts by registered users to access online services of the SP sites, said authenticating comprising accessing the database to verify user account information;

(b) retrieving user-specific access rights data from the database in response to requests from the SP sites and transmitting the access rights data to the SP sites, the access rights data specifying a plurality of content categories or services to which a registered user has access and enabling the SP sites to provide customized access rights to the registered users; and

(c) generating an anonymous ID of a registered user for use by the SP sites and communicating the identifying information for correlating the anonymous ID with an identification of an account of a registered user to the online brokerage site.

72. (Previously Presented) An online brokering service as in claim 71, wherein at least one of the online broker software package and registration software package further performs the function of:

retrieving user-specific customization data from the database in response to requests from the SP sites and transmitting the customization data to the SP sites, the customization data indicating user specified preferences for enabling the SP sites to provide user customized online services.

73. (Previously Presented) An online brokering service as in claim 71, wherein the billing system comprises a software module for allowing the registered user to remotely access an online billing statement, the online billing statement reflecting billing events received by the online broker site from multiple different SP sites.

74. (Previously Presented) An online brokering service as in claim 71, wherein the public network comprises the Internet.

75. (Previously Presented) A virtual online services network for allowing users to directly access service provider (SP) sites over a public network, comprising:

an online brokering service running on at least one site of a computer network, the online brokering service storing billing information for a plurality of users of the public network, the online brokering service providing online access by the users to account-specific billing information;

a registration service running on at least one site of a computer network, and being separate from the online brokering service, the registration service storing account information for a plurality of users of the public network, each of the users having a respective account with the online brokering service;

a plurality of fee-based online services running on a plurality of independent service provider (SP) sites on the public network, the SP sites directly accessible to the users over the public network, each SP site being registered with the online brokering service and the registration service, and being configured to use the registration service to authenticate the users when the users connect to the SP sites over the public network, the fee-based services configured to generate account-specific billing events in response to uses of the online services by the users and to forward the billing events to the online brokering service so that the users are billed for the online services from a centralized billing location; and

a log-on protocol which allows the users to access the plurality of online services using their respective accounts, the log-on protocol configured to (1) prompt a user for an account identifier, (2) cache the account identifier during the course of a user log-on session, and (3) use the cached account identifier to access multiple different SP sites, the log-on protocol thereby allowing the user to seamlessly access the plurality of fee-based online services following a single log-on event;

wherein the registration service stores user-specific access rights data, and provides the access rights data specifying access rights for a plurality of online services for a specific user to the SP sites in response to requests from the SP sites, and wherein the fee-based online services are configured to use the access rights data to automatically provide user-customized services to the users.

76. (Previously Presented) A virtual online services network as in claim 75, wherein the log-on protocol is implemented by respective software components stored on (1) the SP sites, (2) the at least one site of the registration service, and (3) computers of the users.

77. (Previously Presented) A virtual online services network as in claim 75, wherein the log-on protocol includes a challenge-response authentication protocol for allowing the SP sites to authenticate the users.

78. (Previously Presented) A virtual online services network as in claim 75, wherein the public network comprises the Internet.

79. (Previously Presented) An apparatus comprising:

- a broker server operatively connected to a computer network, the broker server having a processor and a computer readable memory, the memory storing broker server implementation software, including customer access software, and at least one broker data structure;
- a registration server operatively connected to a computer network, maintained separately from the broker server, the registration server having a processor and a computer readable memory, the memory storing registration server implementation software, including customer access software, and at least one registration data structure;
- the at least one broker data structure including a list ID and account information for a plurality of registered customers;
- the at least one registration data structure including registration data of a plurality of a plurality of registered customers, the at least one data structure further comprising access rights relating to a plurality of online services;
- whereby the registration server facilitates seamless connection between a selected registered customer and an online site to create a virtual online service, including anonymously providing the selected customer's access rights to the plurality of online services provided by the selected online site, and
- whereby the broker server receives anonymous accounting information from the online site for charges of a customer and receives identifying information from the registration server to permit updating of account information for a respective registered customer.

80. (Previously Presented) An apparatus as in claim 79, wherein the computer network is a public network which comprises the Internet, and wherein the online sites are World Wide Web sites of the Internet.

81. (Previously Presented) A system, comprising:

- (a) a plurality of separate user registration databases, each storing a plurality of user identifications, including user account reference information;
- (b) a provider interface, through which a plurality of providers issue requests to post a transaction to a particular user account, without requiring knowledge of a respective user identity;
- (c) a settlement server, receiving said requests, accessing at least one of said user registration databases, and communicating said request and an user identity to one of a plurality of user account databases; and
- (d) said user registration databases and said user account databases being independent and remotely located with respect to each other.

82. (Previously Presented) A method, comprising:

- (a) recording a user identification, including user account reference information, into one of a plurality of separately maintained user registration databases;
- (b) issuing a request to post a transaction to a particular user account, without requiring knowledge of a respective user identity by a posting party;
- (c) at a settlement server:
 - (i) receiving the request from the posting party,
 - (ii) accessing at least one of the user registration databases, and
 - (iii) communicating the request and an user identity to corresponding one of a plurality of user account databases; and
- (d) independently maintaining the user registration databases and the user account databases at remote locations.

83. (Previously Presented) The system according to claim 1, wherein the token is valid for a restricted period of time.

84. (Previously Presented) The method according to claim 18, wherein said verifying that the client has authenticated at his home provider, and determining that client's access privileges and criteria, is limited in validity for a restricted period of time.

85. (Previously Presented) The method according to claim 35, wherein said verification message is limited in validity for a restricted period of time.

86. (Previously Presented) The method according to claim 49, wherein said verifying step determines whether the authentication message has expired.

87. (Previously Presented) The system according to claim 63, wherein the authentication protocol limits a validity of authentication of registered users for a restricted period of time.

88. (Previously Presented) The system according to claim 69, wherein the verification message is valid for a restricted period of time.